Amendments to the Drawings

The attached drawing sheets include changes to Figures 2B and 3B, and replace the original drawing sheets for Figures 2B and 3B. The changes to the drawings are explained in detail below.

Attachments: Replacement Sheets for Figures 2B and 3B; and
Annotated Sheets Showing Changes to Figures 2B and 3B.

REMARKS

This Amendment is responsive to the Office Action mailed on February 3, 2005. Claims 1, 11, 13, 20, 21, 25, 44, and 48 are amended. Claims 5 and 29 are cancelled. Claims 1-4, 6-28, and 27-48 are pending.

The specification is amended herein to correct various typographical errors, which are apparent from the remainder of the specification and the drawings.

Figures 2B and 3B are amended herein to correct typographical errors therein. In particular, the outputs of shift register 130 (register C) should be designated as "RGC" rather than "RGA" (see, e.g., Applicants' specification, page 14, lines 16-21). Figures 2B and 3B are amended accordingly.

Claims 20 and 44 are objected to based on informalities in the claims. Claims 20 and 44 are amended herein to overcome this objection, withdrawal of which is respectfully requested.

Claims 1-48 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Brown (US 4,860,353) in view of Schneier ("Applied Cryptography, Protocols, Algorithms, and Source Code in C").

Applicants respectfully traverse these rejections in view of the amended claims and the following comments.

Discussion of Amended Claims

Claim 1 is amended to include the subject matter of claim 5. Claim 5 is cancelled to avoid duplication of claimed subject matter.

Claims 11, 13, 20, and 21 are amended to change "third" to --final-- in order to better define Applicants' invention. Claims 20 and 44 are amended to overcome the informality objections raised by the Examiner.

Claim 25 is amended to include the subject matter of claim 29. Claim 29 is cancelled to avoid duplication of claimed subject matter.

Claim 48 is amended to depend from claim 47, to provide proper antecedent basis for the "shared seed input".

Discussion of Prior Art

The Examiner has rejected the pending claims as being unpatentable over Brown in view of Schneier. Applicants' independent claims 1 and 25 are amended herein to include the subject matter of claims 5 and 29, respectively. Accordingly, independent claims 1 and 25 now specify that the feedback shift registers comprise a plurality of dynamic feedback shift registers and at least one static feedback shift register.

The Examiner relies on the disclosure of Brown in rejecting claims 5 and 29 (now included in claims 1 and 25). The Brown patent is owned by General Instrument Corporation ("General Instrument"), the assignee of the present invention. Brown is discussed in Applicants' specification at page 2, lines 19-25 and page 3, lines 18-26.

Brown discloses a dynamic feedback arrangement scrambling technique, commonly referred to by General Instrument as DFAST. DFAST utilizes a single dynamic feedback shift register, the structure of which is varied by a polynomial code signal. The polynomial code signal is varied in accordance with the content of data bits shifted from a predetermined register stage of the feedback shift register (Col. 1, line 50 through Col. 2, line 3; see also, Applicants' specification, page 2, lines 19-26).

Applicants' claimed invention is actually an extension and improvement of the DFAST technology described in the commonly owned Brown patent, and is referred to by General Instrument as DFAST2. Applicants' claimed invention provides a keystream with enhanced cryptographic and ease-of-implementation features as compared to the DFAST technology disclosed in Brown. By using multiple feedback shift registers and multiple randomization (permutation) stages, an enhanced (stronger) cryptographic key is obtained (see, e.g., Applicants' specification, page 3, lines 1-26).

Brown discloses only a single dynamic feedback shift register 10 and a single static feedback shift register 12. In contrast, Applicants' invention as claimed in claims 1 and 25 specifies a plurality of dynamic feedback shift registers and at least one static feedback shift register. By using a plurality of dynamic feedback shift registers and at least one static feedback shift register, and providing data bits from predetermined register stages of each shift register to

randomization stages which permutate the data bits, a very strong keystream is generated. The keystream of Brown is generated using only a single dynamic feedback shift register 10 and a single static feedback shift register 12, without any randomization stages. Accordingly, the keystream generated with Applicants' claimed invention is much stronger than that generated by Brown.

Brown does not disclose or remotely suggest a method or apparatus for generating a keystream using a plurality of dynamic feedback shift registers, as set forth in Applicants' amended claims 1 and 25. Brown discloses only the use of a single dynamic feedback shift register. In addition, there is no disclosure or remote suggestion in Brown to use multiple randomization stages for permutating data bits from predetermined register stages of the shift registers, as claimed by Applicants. Further, there is no disclosure or remote suggestion in Brown regarding the use of a plurality of shift registers together with a plurality of randomization stages as claimed by Applicants.

The Examiner has acknowledged that Brown does not disclose that data bits are permutated at each of several randomization stages. The Examiner relies on Schneier as disclosing permutation techniques (Office Action, page 3). Schneier discloses only permutation as a diffusion technique used to dissipate redundancy of plaintext by spreading it out over the cyphertext. There is no disclosure in Schneier as to how to achieve diffusion, and in particular there is no disclosure of permutating data bits at a plurality of randomization stages, where the data bits are received from predetermined register stages of a plurality of dynamic feedback shift registers and at least one static feedback shift register, as claimed by Applicants.

With Applicants claimed invention, data bits from predetermined shift registers of the plurality of dynamic feedback shift registers and at least one static feedback shift register are provided to a first randomization stage. The output of the first randomization stage is provided to a second randomization stage. The output of the second randomization stage, together with data bits from other predetermined register stages of the feedback shift registers (i.e., the plurality of dynamic feedback shift registers and the at least one static feedback shift register) is provided to at least one additional randomization stage. The data bits are permutated at each randomization stage, and the output of a final randomization stage provides the keystream. There is no

disclosure or suggestion in either Brown or Schneier of such a scheme for generating a keystream.

Only with hindsight impermissibly gained from Applicants' disclosure could one of ordinary skill in the art arrive at the conclusions reached by the Examiner. Brown does not disclose or suggest the use of a plurality of dynamic feedback shift registers, or the use of multiple randomization stages (e.g., first, second, additional, and final randomization stages as claimed by Applicants). Brown does not disclose or suggest any type of permutation of the data bits. Schneier discloses only permutation of data bits, but not permutation of data bits from predetermined register stages of a plurality of shift registers at several randomization stages, as claimed by Applicants.

Further, there is no motivation for one skilled in the art to combine the permutation disclosed in Schneier with the disclosure of Brown, as Brown does not disclose the use of any randomization stages. As indicated in Schneier, there are many ways to obscure redundancies in plaintext, and permutation is only one of them (Schneier, page 237).

In addition, assuming *arguendo* that one skilled in the art would be motivated to combine Brown and Schneier as suggested by the Examiner, one skilled in the art would not arrive at Applicants' claimed invention. Neither Brown nor Schneier disclose or suggest the use of a plurality of dynamic feedback shift registers. In addition, neither Brown nor Schneier disclose or suggest providing data bits from predetermined register stages of multiple feedback shift registers (i.e., the plurality of dynamic feedback shift registers and the at least one static feedback shift register) to multiple randomization stages as set forth in Applicants' claims. By combining Brown and Schneier, one skilled in the art would *perhaps* arrive at a scheme for permutating the data bits that form the pre-keystream 42 of Brown. However, there is no suggestion or motivation to be found in either reference of permutating data bits from predetermined shift registers of multiple shift registers at multiple randomization stages or of providing the output of one permutation stage to another permutation stage, as claimed by Applicants.

Applicants respectfully submit that the present invention as set forth in independent claims 1 and 25 would not have been obvious to one skilled in the art in view of the combination of Brown and Schneier, or any of the other prior art of record.

The foregoing arguments apply equally to Applicants' dependent claims 6 and 30, which specify first and second dynamic feedback shift registers.

Further remarks regarding the asserted relationship between Applicants' claims and the prior art are not deemed necessary, in view of the foregoing discussion. Applicants' silence as to any of the Examiner's comments is not indicative of an acquiescence to the stated grounds of rejection.

Withdrawal of the rejections under 35 U.S.C. § 103(a) is therefore respectfully requested.

Conclusion

The Examiner is respectfully requested to reconsider this application, allow each of the pending claims and to pass this application on to an early issue. If there are any remaining issues that need to be addressed in order to place this application into condition for allowance, the Examiner is requested to telephone Applicants' undersigned attorney.

Respectfully submitted,

Douglas M. McAllister
Attorney for Applicant(s)
Registration No.: 37,886
Lipsitz & McAllister, LLC
755 Main Street
Monroe, CT 06468
(203) 459-0200

ATTORNEY DOCKET NO.: GIC-609
Date: March 15, 2005

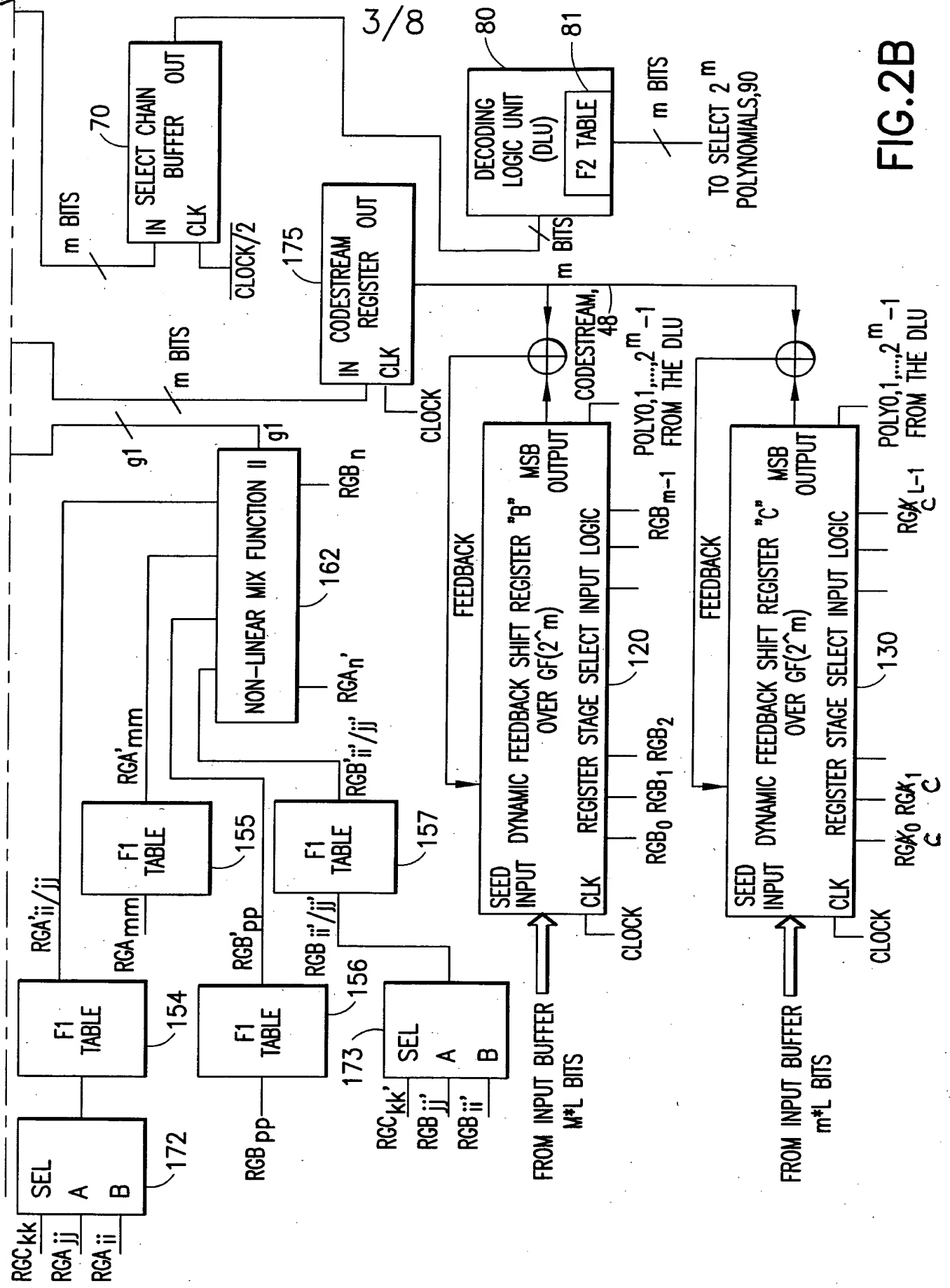

FIG.2B

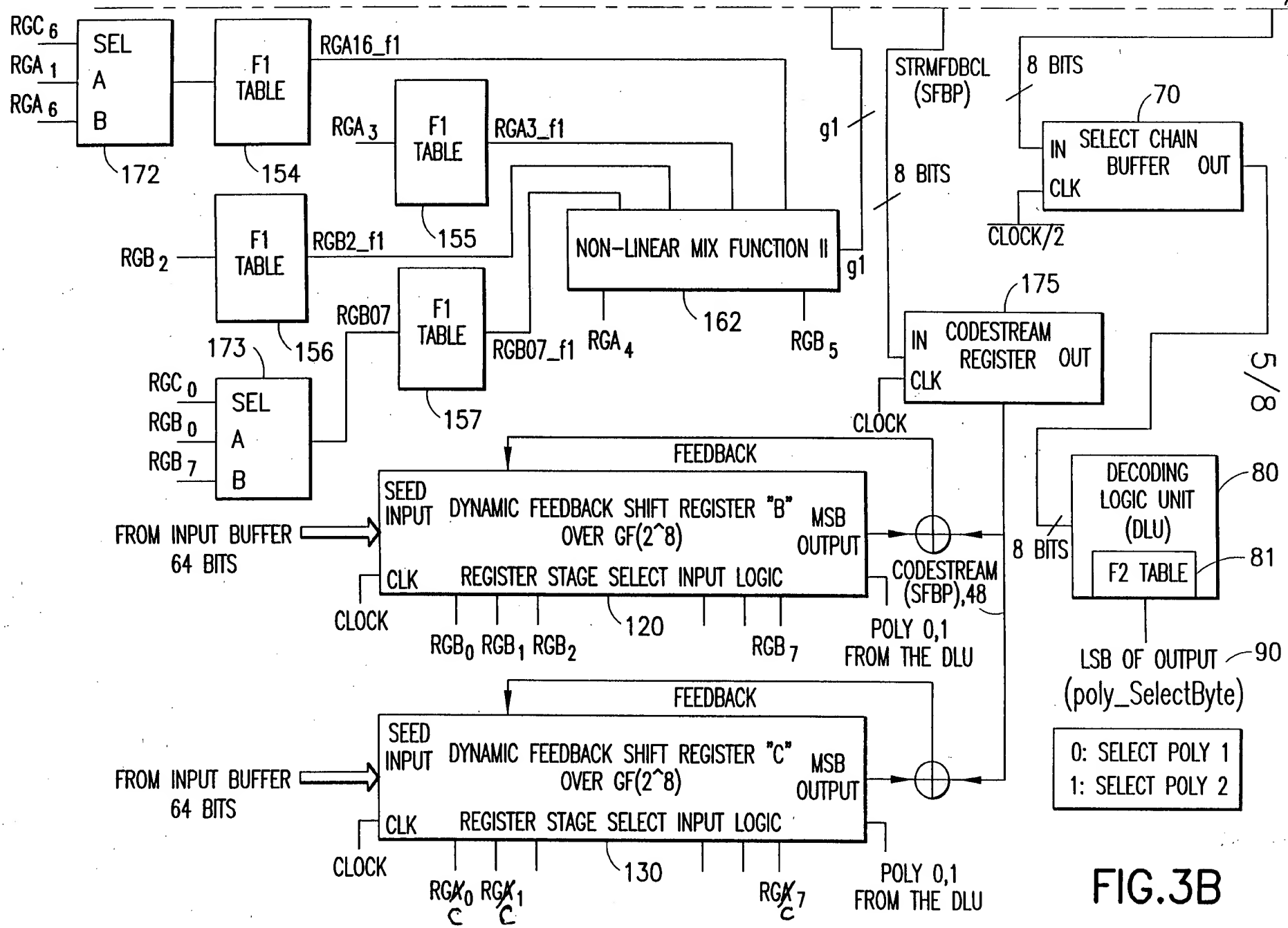

FIG.3B

Application No. 09/717,761
Amdt. dated March 15, 2005
Reply to Office Action of February 3, 2005
ANNOTATED SHEET SHOWING CHANGES